MODERN DEFENSE CIVILIAN PERSONNEL DATA SYSTEM (DCPDS)

DEPLOYMENT PLAN

Prepared by

Defense Civilian Personnel Management Service

May 15, 2000

TABLE OF CONTENTS

1. PURPOSE 1
1.1 Deployment Definition 1
1.2 References to Other Documents 1
2. BACKGROUND 1
3. DEPLOYMENT IMPLEMENTATION ROLES AND RESPONSIBILITIES 1
3.1 Civilian Personnel Management Service (CPMS) 1
3.2 Technical Oversight 2
3.3 DoD Components 2
3.3.1 Deployment Preparation 2
3.3.2 Deployment Site Participants 3
3.3.3 Deployment POCs 3
3.3.4 Deployment POC Program Areas 3
4. DEPLOYMENT STRATEGY 7
4.1 Incremental Deployment 7
4.2 Scope of Deployment 7
4.3 Deployment Commencement 8
4.4 Deployment Duration 8
4.5 System Downtime During Deployment 8
4.6 Extended Deployment Duration 9
4.7 Modern DCPDS Installation 9
4.8 On-site Deployment Teams 9
4.8.1 CPMS Deployment Team Responsibilities. 10
4.8.2 Technical Contractor Deployment Team Responsibilities. 11
4.8.3 Component Deployment Responsibilities. 11
4.8.4 RESUMIX Deployment Responsibilities. 12
4.9 Deployment Milestones 13
4.10 Deployment Schedule Reporting Requirements 14
4.11 Deployment Schedule Changes 14
4.12 Advanced Equipment Readiness 15
5. PREDEPLOYMENT PREPARATION 15
5.1 Planning 15
5.2 Site Preparation 16
5.2.1 Facility Requirements 16
5.2.2 System Support Requirements (Hardware, Software, & Communication) 17
5.3 Deployment Working Group 18
5.3.1 Purpose of Deployment Working Group 18
5.3.2 Working Group Composition 18
5.3.3 Information Exchange 18
6. MIGRATION FROM LEGACY DCPDS TO MODERN DCPDS 18
6.1 Legacy DCPDS and PPI Suite Deactivation 18
6.2 Termination of Legacy DCPDS Operational Support 19
6.3 Contingency Plans 19

6.4 Partial Deployment of Modern DCPDS 20
7. PERSONNEL ACTIONS MORATORIUM 20
7.1 Controllable Projected Personnel Actions Pending in Legacy DCPDS at Time of Deployment 20
7.2 Processing Emergency Personnel Actions During Deployment 21
7.3 Uncontrollable Personnel Actions Pending in Legacy DCPDS During Deployment 24
7.4 SF-52 Pipeline Actions Unconsummated in PERSACTION 24
7.5 Vacant Position Data 24
8. TRAINING 24
9. DATA CONVERSION 25
9.1 Data Conversion to Modern DCPDS 25
9.2 Advanced Data Validation 25
9.3 Status Six Records 25
9.4 Data Validation During Deployment 25
9.5 Hierarchy Data in Modern DCPDS 26
9.5.1 Hierarchy Data Structure 26
9.5.2 Organization Hierarchy Data Maintenance 26
9.5.3 Position Hierarchy Data Maintenance 26
9.5.4 Military Position Hierarchy Data 27
9.6 Historical Data 27
9.6.1 Historical Data Capture 27
9.6.2 Historical Data Conversion 27
10. CONFIGURATION MANAGEMENT (CM) 27
10.1 Changes to Operating System Hardware or Software 28
10.2 Operating System Software Version Control 28
11. SECURITY 28
11.1 Security Goals 28
11.2 Security References 29
11.3 User Access to Modern DCPDS 29
11.3.1 Preparation for User Access to Data in the Modern DCPDS 29
11.3.2 User Access to the Corporate Management Information System (CMIS) 30
11.4 Preparation for CMIS Security Administrator Accounts and User Security Training 30
11.5 Component Initial User Access Required Actions 30
11.6 Certification and Accreditation at RSC and CSU Sites 30
12. DEPLOYMENT PLAN MAINTENANCE 30
13. DOCUMENTS REFERENCED IN DEPLOYMENT PLAN 31
APPENDIX A – SAMPLE DEPLOYMENT DURING ANY MONTH 32
APPENDIX B – GLOSSARY OF TERMS AND ABBREVIATIONS 33
APPENDIX C – TECHNICAL DEPLOYMENT STRATEGY 35
1. Introduction 35
2. Purpose 35
3. Scope 35
4. Risk Identification 35
5. Technical Deployment Strategy 35
6. Processing Sequence 36

7. Wrapper Definition 36
8. Data Reject Handling 36
9. Deployment 38
10. Detail Specifications 38
11. Legacy History Data Conversion 38

1. PURPOSE

This plan identifies the high-level requirements and sequence of events necessary to convert Department of Defense (DoD) Component Regional Service Centers (RSCs) from the legacy DCPDS to the modern DCPDS in a timely and orderly manner. When reference is made throughout this plan to the modern DCPDS it includes Oracle Human Resources (HR), Oracle Training Administration (OTA), RESUMIX, the Corporate Management Information System (CMIS), and associated software and databases.

1.1 Deployment Definition

Deployment consists of all actions necessary to distribute and implement the modern DCPDS and associated hardware and communications across DoD. Deployment includes, but is not limited to modern DCPDS software distribution, software and hardware configuration, data capture, conversion, upload, training, and post evaluation. Hardware and communications are being established through the DoD Regionalization Program. Please refer to the DCPDS Modernization Program Concept of Operations (CONOPS) for additional information on general system characteristics, the provision of centralized operations, and the concept of maintenance support for the modern DCPDS.

1.2 References to Other Documents

This deployment plan makes references to other documents, system plans, guides, and schedules. These references are made to maintain the brevity of this plan and yet ensure adherence to all of the requirements that are critical to the successful preparation, configuration, distribution, training, security, and installation of the modern DCPDS. This plan provides essential planning information and addresses critical implementation considerations that will ensure a successful deployment of the modern DCPDS with minimal disruption to the end user.

2. BACKGROUND

The DCPDS Modernization Program is top-down directed by authority of Program Budget Decision (PBD) 711, dated 5 December 1994. The objective of the Modernization Program is to replace the existing legacy personnel data system with a robust relational database, client/server environment that is significantly more responsive to the unique processing and information requirements of regionalized and downsized civilian personnel offices throughout DoD. This direction is driven by the need to support DoD's Regionalization Program in response to Defense Management Report Decision (DMRD) 906, and the November 1993 Program Decision Memorandum (PDM).

3. DEPLOYMENT IMPLEMENTATION ROLES AND RESPONSIBILITIES

3.1 Civilian Personnel Management Service (CPMS)

CPMS has the overall program management responsibility for planning, coordination, oversight, and execution of the modern DCPDS deployment program as prescribed by this plan. CPMS monitors and assesses site readiness, deployment status, affect of associated problems, and proposed changes. CPMS will also augment, within time and staff limitations, Component site training, and will send on-site teams to deploy the modern DCPDS. CPMS will review and approve the Component modern DCPDS deployment schedules to determine possible conflicts with other deployment schedules, compliance with overall DoD deployment milestones and requirements, and the availability of CPMS staff needed to provide remote and on-site operational assistance to the deployment sites. CPMS will prepare a master, integrated DoD deployment schedule based on input from all the Components. CPMS will also review Component Technical Implementation Plans, and Component-unique requirements and deployment schedules to determine the readiness of each deployment site, and whether there are any potential problems.

3.2 Technical Oversight

The technical contractor has technical oversight and responsibility for the deployment of the modern DCPDS to all DoD agencies including data conversion and associated processes. The technical contractor will prepare all source files that are required to be loaded at the user sites. The technical contractor is responsible for software configuration management to ensure the correct version of the modern DCPDS software is deployed to the user sites including identification of the correct operating system version needed to operate the modern DCPDS platform. The technical contractor will provide on-site deployment technical assistance teams to deploy the modern DCPDS. The technical contractor will review the Component modern DCPDS deployment schedules, in coordination with CPMS, to determine conflicts with other deployment schedules, and the availability of technical staff needed to provide remote and on-site technical and system installation assistance to the deployment sites. The technical contractor will also review the Component Technical Implementation Plans to determine the readiness of each deployment site.

3.3 DoD Components

3.3.1 Deployment Preparation

The DoD Components retain responsibility for funding, planning, scheduling, and implementing their own Component-unique site preparation requirements necessary to facilitate the modern DCPDS deployment including deployment to their civilian employee, manager, and commander workstations. Most, if not all, site preparatory actions should have occurred for each deployment site by the time this deployment plan is implemented. However, to reinforce the importance of proper site preparation, the deployment POCs are reminded to consider the specific deployment program areas listed below, at a minimum, to properly prepare the Regional Service Centers (RSCs), Customer Support Units (CSUs), and satellite personnel offices for deployment. DoD Components are responsible for determining their facility requirements and for acquiring their own equipment and non-application software needed to support the modern DCPDS. Components will fund and staff their own site-specific facility acquisition and preparation, including training. Responsibility for modern DCPDS deployment to the manager workstations must remain with the Components for a number of valid reasons in addition to DCPDS Modernization Program funding restrictions. Limited CPMS, technical contractor, and Component staff resources restrict the size and number of deployment teams to deploy the modern DCPDS to numerous civilian personnel sites within a short period of time. Deployment teams are required to meet the Components back-to-back deployment schedule for all of their deployment sites within the predefined overall deployment milestones. As a result**,** the teams are severely limited in providing any extended assistance.

3.3.2 Deployment Site Participants

Deployment of the modern DCPDS requires the full support and cooperation of many representatives from the Components as well as those from CPMS and the technical contractor. Components must ensure that designated deployment POCs for each RSC (the RSC POC represents the CSUs and satellite personnel offices in their region) are on duty and available during deployment to facilitate all associated local efforts (such as those listed in paragraph 3.3.4 below) within their respective region including their RSC and assigned CSUs and satellite personnel offices. The CSU and satellite personnel office deployment POCs should be on duty and available during deployment to coordinate their required actions with their respective RSC deployment POCs. Components are encouraged to use their “in-house” or contracted staff to maximize the augmentation of on-site deployment teams containing CPMS and technical contractor representatives.

3.3.3 Deployment POCs

Components should identify modern DCPDS deployment POCs down to the RSC level, at a minimum, and preferably to the CSU level, for each of the program areas listed below. Examples of duties for these contacts should include, but are not limited to, coordination of system functional matters with CPMS deployment POCs, and coordination with the technical contractor on such matters as software installation, system administration, hardware configuration, system and data interfaces, data conversion, training, and related matters. The deployment POCs are responsible for tracking the status of their assigned modern DCPDS program areas. Deployment POCs must be identified in the deployment schedule submitted to CPMS (See paragraph 4.10 Deployment Schedule Reporting Requirements). CPMS expects many, if not most, of these local deployment responsibilities to be assigned on the basis of available staff and their training, skills, and experience with modern DCPDS operation and software deployment processes.

3.3.4 Deployment POC Program Areas

3.3.4.1 Planning

3.3.4.1.1 Establish a single point of contact for scheduling and coordinating all local modern DCPDS deployment matters.

3.3.4.1.2 Determine optimal method to monitor and manage personnel action processing with the modern DCPDS. Develop troubleshooting procedures for potential and known problem areas.

3.3.4.1.3 Ensure overall modern DCPDS operational readiness.

3.3.4.1.4 Oversee budget, funding, and local site preparation and hardware purchases needed for modern DCPDS deployment. This may be assigned as a separate responsibility or combined with overall planning POC duties.

3.3.4.1.5 Ensure all modern DCPDS administration documentation required for local reference purposes is available and sufficient copies of the system operating documentation are available for the local users.

3.3.4.2 Facility Readiness Status Reviews and Reports

3.3.4.2.1 Oversee all facility renovation efforts and report on readiness to support new server, workstations, and communications equipment associated with the modern DCPDS. Refer to your Component Technical Implementation Plans.

3.3.4.2.2 Track and report status of facility readiness to the Component deployment POC.

3.3.4.3 Acquisition Document Control

3.3.4.3.1 Verify all documents necessary to order or purchase hardware, systems software, communications, and facility renovation materials. Refer to the Technical Implementation Plans for consistency of items ordered.

3.3.4.4 Training

3.3.4.4.1 Ensure all local modern DCPDS and CMIS user training requirements are surveyed, identified, and met in accordance with the Training Support Plan (TSP) requirements.

3.3.4.4.2 Request CPMS training support regarding such areas as embedded and computer-based training, train-thetrainer instruction, training strategies, and related matters to minimize Component and local training development and material costs.

3.3.4.5 Database Administration

(Refer to the CONOPS.)

3.3.4.5.1 Establish user access procedures.

3.3.4.5.2 Monitor the system for database problems and either resolve them or bring them to the attention of the appropriate action officer for resolution.

3.3.4.6 Systems Administration

(Refer to the CONOPS.)

3.3.4.6.1 Confirm appropriate system configuration of affected platforms such as disk space or directory structure with system configuration recommended by the technical contractor.

3.3.4.6.2 Maintain roles and responsibility data for modern DCPDS and CMIS user access including user identification designators (IDs) and passwords.

3.3.4.6.3 Facilitate system configuration changes as applicable.

3.3.4.6.4 Manage system resources to optimize processing.

3.3.4.6.5 Address problems as they arise and immediately report them through designated channels if they affect the modern DCPDS deployment schedule.

3.3.4.6.6 Conduct system testing to determine readiness at local site.

3.3.4.6.7 Ensure local modern DCPDS users are apprised of new procedures.

3.3.4.6.8 Maintain close liaison on software distribution and installation matters with the technical contractor.

3.3.4.6.9 Coordinate software installation on-site.

3.3.4.6.10 Oversee plan for local modern DCPDS deployment to affected users.

3.3.4.6.11 Provide local system customer assistance and troubleshooting assistance to modern DCPDS users as required.

3.3.4.6.12 Report daily modern DCPDS installation status to CPMS and Component deployment POCs.

3.3.4.6.13 Assign related responsibilities to RSC system administration POCs as required for associated CSU and satellite personnel offices.

3.3.4.6.14 Coordinate with the technical contractor for conversion of local data from the legacy DCPDS data format to the modern DCPDS data structure including data capture and validation, if necessary.

3.3.4.6.15 Ensure Component or RSC system administration POCs coordinate with the technical contractor on such matters as problems with conversion of local data from the legacy DCPDS to the CMIS, and to the modern DCPDS.

3.3.4.7 Computer and Communications Acquisition and Installation

(The Components' Technical Implementation Plans for regionalization provide details for configuration of hardware and communications. Also refer to the CONOPS.)

3.3.4.7.1 Conduct survey and compile list of modern DCPDS users and build a connectivity profile for each.

3.3.4.7.2 Coordinate communications infrastructure and connectivity issues needed to support the modern DCPDS. Work with appropriate communication Office of Primary Responsibility (OPR) to facilitate linking modern DCPDS users within and outside the personnel office.

3.3.4.7.3 Coordinate computer configuration, acquisition, and installation requirements based on modern DCPDS user requirements within and outside the personnel office.

3.3.4.7.4 Ensure there are no communications exercises, repairs, or similar activities scheduled to occur that would disrupt the deployment and validation of the modern DCPDS at those sites.

3.3.4.8 System Software and Hardware Maintenance

Determine and oversee requirements and contracts needed for maintenance of systems software and hardware supporting the modern DCPDS. (See the Maintenance Support Plan for associated details.)

3.3.4.9 Configuration Management

3.3.4.9.1 Coordinate local configuration management matters. See the Configuration Management Plan for associated details.

3.3.4.9.2 Centrally manage the modern DCPDS software inventory for local site, including systems software , based on the configuration management standards and specifications determined by the technical contractor.

3.3.4.10 Security

Monitor site security arrangements for compliance. Resolve security issues as necessary. (See the Security Support Plan for associated details.)

4. DEPLOYMENT STRATEGY

4.1 Incremental Deployment

Modern DCPDS deployment will be conducted incrementally to meet the Initial Operating Capability (IOC) and Full Operating Capability (FOC) requirements of each DoD Component beginning in October 1999. First deployment of the modern DCPDS will be to three designated Operational Test and Evaluation (OT&E) sites. The modern DCPDS will be deployed to sites that have regionalized. Those sites still pending regionalization when deployment begins will follow the Component Technical Implementation Plans for setup, which includes a site survey and certification approval process. It is expected that all DoD sites will be converted to the modern DCPDS beginning in 2000. Deployment scheduling, sequencing, preparation, execution, and reporting required by this deployment plan will take into consideration each Component's unique regionalization configuration. These factors include varying scope of support, size, structure, site readiness, and geographical dispersion of each Component's RSCs, CSUs, and satellite personnel offices in accordance with their respective Technical Implementation Plans for regionalization.

4.2 Scope of Deployment

Approved program funding for the DCPDS Modernization Program through PBD 711 supports only direct civilian human resources operations. Consequently, since its inception, the primary focus of the DCPDS Modernization Program has been to replace the legacy DCPDS with a modern automated civilian personnel information system that will better support the DoD Components' headquarters and regionalized civilian personnel offices. PBD 711 and DMRD 906 do not provide approved program funding for hardware, communications, hardware maintenance, training, or deployment of the modern DCPDS to the manager and employee levels. Deployment of the modern DCPDS to the manager and employee operational levels is the responsibility of the Components. However, the technical contractor will advise, when possible within the constraints of its available time and technical staff, on Component use of automated software distribution tools to remotely deploy the modern DCPDS to the manager and civilian employee workstations.

4.3 Deployment Commencement

Commencement of the modern DCPDS deployment to a region will occur the first Friday of a designated two-week pay period. Component deployment schedules for each site must reflect this deployment-scheduling requirement. Components should ensure the availability of their local staff to assist in deployment, other Component staff needed to provide on-site deployment assistance at other sites, and the readiness of their equipment. CPMS and the technical contractor will review these deployment schedules to determine conflicts with other Component deployment schedules, and availability of equipment and staff for on-site deployment assistance. Components are cautioned that selection of deployment dates going beyond or overlapping the end of a month could cause some reporting anomalies for end-of-month reporting since some data may not be obtainable.

4.4 Deployment Duration

Components should plan on a duration of two weeks for modern DCPDS deployment to each region. Deployment to the first OT&E site may be longer to ensure stability of the system. This includes installation of the software, data conversion, and all other associated deployment actions for their respective RSCs, CSUs, and satellite personnel offices. During development of the Deployment Program, the two-week deployment period of time was identified as an initial estimate for the maximum permissible downtime period. This does not mean the deployment period will actually be two weeks in length. The scheduled two-week deployment period of time for software installation, data conversion, local system testing, and all other related actions must begin the week before a two-week pay period. This deployment scheduling requirement permits the deployment site to process an end-of-day (EOD) on Thursday before deployment begins. The EOD would be effective the next day, Friday. Upon completion of that EOD action, the deployment site can process a forced EOD effective the Friday of the next week. A payroll file then can be transmitted to the servicing payroll office on the EOD effective date. Deployment teams will stay on-site at each region until the modern DCPDS is operational.

4.5 System Downtime During Deployment

The modern DCPDS deployment program objective is to deploy the modern DCPDS to the regions with minimum downtime. During the two-week deployment downtime, the region must cease use of the legacy DCPDS, including the PPI suite, when the modern DCPDS is installed at the affected region and certified as fully operational. All timesaving measures will be used in the data conversion and system installation processes to minimize the downtime period to the fullest extent possible and to decrease any further inconvenience to local personnel operations.

4.6 Extended Deployment Duration

Components should develop contingency plans to cover unforeseen problems requiring additional deployment time. Since any deployment extension will delay automated personnel action processing for such regions (See paragraph 6, Migration from legacy DCPDS to modern DCPDS, for details on contingency plans, and paragraph 7, Personnel Action Moratorium, for details on curtailment of personnel action processing during deployment). Components must explain in the deployment schedules that they submit to CPMS, for incorporation into the DoD master deployment schedule, any anticipated problems that will increase the deployment duration beyond the expected two-week deployment period for any region.

4.7 Modern DCPDS Installation

The technical contractor will be responsible for installing the modern DCPDS at each RSC in accordance with the Component deployment schedule. On-site deployment teams will install the modern DCPDS at each region. The composition of the on-site deployment team is described in the next section of this document. When the modern DCPDS is deployed to a region, all sites within the respective region, including the RSC and each assigned CSU, will receive the system concurrently. Exceptions to simultaneously deploying the modern DCPDS to the RSC and assigned CSUs and satellite personnel offices must be documented in the Component's deployment schedule for planning and rescheduling purposes, including information on supporting computer system and alternate communication connections where applicable. While the deployment teams will primarily be sent to provide region-wide software installation, some CSUs may require assistance with on-site loading of the software due to a lack of local expertise, size, complexity, or problems with the local computer equipment and communications. However, it is expected that the Components will support such requirements.

4.8 On-site Deployment Teams

Deployment teams will consist of technical and functional personnel from CPMS, the technical contractor, and the Components. RESUMIX technical representatives will normally install the RESUMIX software and convert customized data, where applicable, before deployment of the modern DCPDS. RESUMIX technical representatives will be on standby status to provide assistance as necessary during deployment of the modern DCPDS. Components are responsible for determining the sources and number of their augmentees for the deployment teams based on their availability, skills, experience, and level of support needed at the RSCs during deployment. Support of all modern DCPDS deployment to the CSUs and satellite personnel offices will be provided remotely from their respective RSC. Deployment teams will not be sent to any CSU or satellite personnel office to provide on-site deployment or data conversion assistance unless it is absolutely critical to ensure proper deployment. Restricted program funding, short deployment duration, and deployment team staff limitations prevent direct on-site or remote deployment support to the manager and employee levels. Deployment teams will remain on-site at the RSC until the modern DCPDS is fully deployed and operational throughout the region.

4.8.1 CPMS Deployment Team Responsibilities.

- Serve as Deployment Team Leader for both the functional and technical teams.
- Serve as on-site experts and advisors on the personnel functions and operation of the modern DCPDS to ensure its successful deployment and operation throughout the RSC.
- Validate the modern DCPDS at each RSC to ensure the system is fully deployed and operational throughout all associated regional personnel offices.
- Facilitate deployment actions with functional and technical POCs from the technical contractor, Component, and region by applying personnel and modern DCPDS expertise to such matters as the resolution of data conversion problems, explanation of personnel laws and requirements that apply to the functionality of the modern DCPDS, and operation of the new system.
- Evaluate functional and operational deployment progress, associated problems, and plans for solving these problems. Report status to DCPDS Modernization Program Manager.
- Provide desk-side help and coaching as necessary (not training) on modern DCPDS operating procedures to regional staff. Note: Regional staff received sufficient system operation training prior to deployment.
- Provide desk-side help and coaching as necessary (not training) on modern DCPDS functional capabilities to regional staff. Note: Regional staff received sufficient system functional training prior to deployment.
- Ensure that the modern DCPDS installed at the region meets all specified operational and functional requirements and is fully operational before the CPMS deployment team members depart the RSC.
- Conduct exit survey prior to departing the RSC to measure and assess the success of the deployment for application of “lessons learned” to subsequent deployments.
- Evaluate success of training given to personnelists at the region on the functionality and operation of the modern DCPDS.

4.8.2 Technical Contractor Deployment Team Responsibilities.

- Serve as on-site technical experts and advisors on the installation, configuration, and system and database administration of the modern DCPDS to ensure its successful deployment and operation throughout each RSC.
- Ensure the regional hardware and operating system are ready (operation, configuration, etc.) for the installation of the modern DCPDS at each RSC. Troubleshoot the hardware and operating system as necessary.
- Coordinate with the Component and RSC technical staff on computer and operating system requirements for the installation of the modern DCPDS at each RSC.
- Coordinate with Component, local installation, or RSC communications staff on regional communications infrastructure and connectivity issues and requirements necessary to support the operation and interfaces of the modern DCPDS within and outside of the RSC.
- Oversee and conduct installation of modern DCPDS software and database at each RSC.
- Validate modern DCPDS installation and operation at the RSC to ensure all system technical requirements are met throughout the region.
- Evaluate technical deployment progress and problems, and plans for solving these problems.
- Explain, as necessary, modern DCPDS database and system administration procedures and requirements to regional technical staff.
- Ensure that the modern DCPDS installed at each region meets all specified technical requirements and is fully operational before the technical contractor deployment team members depart each RSC.

4.8.3 Component Deployment Responsibilities.

- Serve as primary points of contact for scheduling and coordinating all modern DCPDS deployment matters in the RSC, associated CSUs, and satellite personnel offices.
- Coordinate with the deployment team members to ensure the regional facilities, hardware and operating system software are ready for the installation and operation of the modern DCPDS at the RSC, CSUs, and associated personnel offices.

- Coordinate with the technical contractor deployment team members regarding computer and operating system requirements for the installation of the modern DCPDS at the RSC, CSUs, and associated personnel offices.
- Coordinate with the technical contractor deployment team members regarding security requirements and their effect on the secure operation of the modern DCPDS. Apply knowledge of Component, local, and regional communication infrastructure and connectivity requirements to facilitate the technical contractor's installation and testing of the modern DCPDS throughout the region.
- Conduct tests of modern DCPDS operation on-site at the RSC with technical contractor and CPMS deployment team members to verify system readiness at the RSC and throughout associated CSUs and satellite offices.
- Coordinate with the technical contractor and CPMS deployment team members to ensure the successful conversion of each RSC's database from the legacy to the modern DCPDS format. Assist in the resolution of data conversion problems.
- Coordinate and oversee all modern DCPDS deployment actions with commanders, managers, and employees supported by the RSC personnel offices.
- Ensure all modern DCPDS administration and operation documentation required for local reference purposes is available for the local users.
- Obtain security passes for the DoD Deployment Team members to facilitate their entry to each RSC's installation and RSC facility, if necessary.

4.8.4 RESUMIX Deployment Responsibilities. Note: The following responsibilities regarding RESUMIX deployment will normally be performed prior to the deployment of the modern DCPDS.

- Provide technical experts and advisors on the installation, configuration, and system and database administration of RESUMIX to ensure its successful operation throughout each RSC and associated CSU and satellite offices.
- Ensure the regional hardware and operating system is ready for the installation of RESUMIX. Troubleshoot the hardware and operating system as necessary.

- Coordinate with Component, local installation, or RSC communications staff on regional communications infrastructure and connectivity issues and requirements necessary to support the operation and interfaces of RESUMIX within and outside each RSC.
- Oversee and conduct installation of RESUMIX software and associated database including any customized database at each RSC.
- Test and validate the installation and operation of RESUMIX to ensure all system technical requirements are met throughout each region and that the system is fully operational.
- Explain, as necessary, RESUMIX database and system administration procedures and requirements to regional technical staff. **Note**: Regional staff will receive RESUMIX database and system administration training prior to RESUMIX deployment.

4.9 Deployment Milestones

The overall modern DCPDS deployment milestones are listed below in Table 1. The dates listed are subject to change to meet new deployment requirements. Components will be promptly notified of any deployment milestone changes so they can determine the effect on their deployment schedules and make schedule changes as necessary.

Table 1. MODERN DCPDS DEPLOYMENT MILESTONES

ACTION	PHASE	MILESTONE
Begin modern DCPDS deployment *(OT&E Sites only)**	IOC	October 15, 1999
AFOTEC OFT *(Army only)*	IOC	Nov 29 – Dec 10, 1999
AFOTEC OT&E *(AF and Navy Sites only)**	IOC	Jan 10 – Feb 9, 2000
AFOTEC Report Completed	IOC	April 2000
Pre-Planned Upgrade (PPU)	IOC	May 2000
Milestone III Review and Decision	IOC	May 2000
Start full modern DCPDS deployment	FOC	June 2000
Complete modern DCPDS deployment	FOC	December 2000

*When the modern DCPDS is deployed to the OT&E sites, each OT&E region, including the associated RSC and all assigned CSUs and satellite personnel offices, should be installed with the modern DCPDS. Reference the Consolidated Deployment Schedule for specific deployment dates and sites.

4.10 Deployment Schedule Reporting Requirements

Components should submit to CPMS their deployment schedules for all of their sites for incorporation into the master DoD deployment schedule. The schedules should reflect a two-week deployment duration for each region unless it anticipates problems that will increase the deployment duration. The information required in these schedules is listed in Table 2 below. There is no specific format for the deployment schedules so long as they are orderly and contain the information required. The deployment schedules should be reported only one time through the Component deployment POCs to the CPMS deployment POC. The deployment schedule will serve two requirements. First, CPMS and the technical contractor must be aware of the deployment schedule for each affected site in sufficient time to ensure the availability of functional and technical staff, and associated resources needed to deploy the modern DCPDS on the dates requested by the Component. Second, CPMS and the technical contractor must be given timely notice of the Component deployment schedules to ensure the availability of expert staff for any special requirements. All deployment actions apply to both CONUS and OCONUS modern DCPDS deployment sites. Continuous reviews should be conducted to assess deployment schedules, related schedule changes or problems, and site readiness progress. Component schedules for deployment of the modern DCPDS should contain the following information for each site.

Table 2. DEPLOYMENT SCHEDULE CONTENTS

1. Modern DCPDS deployment dates for each RSC, CSU, and satellite personnel office.
2. Dates on which the Components prefer the deployment not be conducted for any region, e.g., date conflicts with wage studies, holidays, or periods of high workload.
3. Component deployment POC names, phone numbers, and email addresses.
4. Component personnel and technical representatives to augment the CPMS and technical contractor on-site assistance teams.
5. Overall status of facility, computer, server, workstation, and communications readiness. If a site is not ready, state when it will be ready for modern DCPDS deployment.
6. Issues and concerns adversely affecting the modern DCPDS deployment to any RSC, CSU, and satellite personnel office, and reasons for any deployment delay.
7. Component plans for continuing use of legacy system at sites not ready for conversion.

4.11 Deployment Schedule Changes

Component deployment schedules may change as factors and events affecting the site preparation and equipment readiness change. Changes to previously scheduled and reported deployment data should be reported immediately through the Component deployment POCs to the CPMS deployment POC. Timely notification of deployment schedule changes ensures availability of CPMS and deployment contractor staff, and equipment resources needed to support the Component deployment requirements. Components are responsible for making a maximum effort to substitute scheduled sites when delays occur, rather than simply postponing locations. This will help to ensure overall timely deployment and proper utilization of deployment assistance staffs.

4.12 Advanced Equipment Readiness

Components that have not already installed their support equipment should plan their deployment schedules to include equipment installation and readiness no later than one month prior to their scheduled modern DCPDS deployment. While this advanced equipment readiness requires moving the site preparation ahead by the same amount of time, this capability provides several benefits. The user site must have all computer hardware, system software, and associated communication equipment ready to meet the modern DCPDS deployment schedule. This advanced readiness allows for additional familiarity and training time beyond the training already received, as well as additional time to train the local users on the modern DCPDS and associated support equipment on-site. Development of an equipment test plan is recommended to ensure site readiness for installation of the modern DCPDS. This advance preparation will also enhance achievement of higher productivity levels after system deployment in a shorter period of time. Components are encouraged to include in their deployment schedules any risks that could affect the scheduled modern DCPDS deployment to each site. Deployment POCs for each Component, RSC, CSU, and satellite personnel office must ensure the appropriate documentation is on hand for each modern DCPDS deployment site. Documentation should include system administration and operation of the modern DCPDS software as well as instructions for the installation and operation of the supporting equipment and operating system.

5. PREDEPLOYMENT PREPARATION

Provided below are suggested deployment preparation factors for modern DCPDS deployment POCs to consider from Component levels down to the CSUs and satellite personnel offices as they conduct their site preparation activities. This section is not intended to replace Component deployment plans, and does not include all tasks required to prepare for an orderly deployment of the modern DCPDS at any site.

5.1 Planning

Adequate planning for site preparation of each RSC, CSU, and satellite personnel office is crucial to ensuring the sites are ready for deployment of the modern DCPDS as scheduled. “Lessons learned” from previous system deployments, including the interim Personnel Process Improvement (PPI) suite, dictate the need for careful planning and consideration of all details affecting deployment site readiness, equipment size, configuration, acquisition, installation, and testing well in advance of the scheduled deployments. Significant changes to any site assessment and readiness adversely affecting the deployment schedule should be reported immediately through the affected Component to the CPMS deployment POC. Any site readiness change is considered significant if the deployment schedule for the respective site must also be changed. At a minimum, Components should consider developing a well-documented site preparation plan for each RSC, CSU, and satellite personnel office to significantly facilitate the deployment process.

5.2 Site Preparation

This portion of the modern DCPDS deployment plan is intended to emphasize the criticality of proper site preparation for the successful deployment and operation of the modern DCPDS. These preparations require considerable facility and equipment replacement and upgrade since such operations and support equipment are new to most sites. The designated deployment site preparation POCs for the Components, RSCs, CSUs, and satellite personnel offices are encouraged to refer to the Deployment Implementation Guide or the Master Deployment Checklist to help ensure their sites are ready for deployment of the modern DCPDS. Prior to site preparation for deployment of the modern DCPDS and to establishing access to the CMIS, Components must submit a Technical Implementation Plan for their facility and system support equipment requirements (i.e., for each RSC, CSU, and satellite personnel offices). The plan will be reviewed by the technical contractor and approved by CPMS. If a region has not been certified by the technical contractor, the owning Component must determine if the site is ready, and subsequently submit its Technical Implementation Plan and request for regional site certification. Site certification is required for each region (i.e., RSC and all assigned CSUs and satellite personnel offices) before the modern DCPDS can be deployed. Individual personnel offices, functioning as regional equivalents, must be certified before the modern DCPDS can be deployed to those sites. The checklists attached to the January 13, 1997, memorandum from the Acquisition Program Manager on Operational Certification for RSCs and Risk Analysis Status should be used as a guide in preparation for modern DCPDS deployment and operational certification.

5.2.1 Facility Requirements

5.2.1.1 Facility Site Surveys

Each RSC, CSU, and satellite personnel office, where the system support equipment is to be located, should be surveyed to determine requirements such as space, heating, cooling, electrical power, ventilation, and access to the equipment.

5.2.1.2 Facility Renovation Coordination

As outlined in paragraph 3.3.4. above, a POC should be identified for each deployment site to coordinate all overarching facility preparation requirements, schedules (e.g. acquisition, installation, and reports), agreements, and plans necessary to meet the timelines established in advance of the modern DCPDS deployment. Facility POCs at each RSC, CSU, and satellite personnel office must promptly elevate their inability to resolve critical facility preparation problems. Unresolved facility preparation problems are considered critical if they adversely affect the deployment schedule for any site. Any unresolvable problems affecting a previously reported deployment schedule must be reported immediately through designated Component channels to CPMS. CPMS will determine the effect on the overall DoD deployment schedule.

5.2.2 System Support Requirements (Hardware, Software, & Communication)

5.2.2.1 System Support Site Surveys

Careful planning for the system support requirements survey, determination, acquisition, and installation for each modern DCPDS deployment site is critical to ensuring the successful deployment and operation of the modern DCPDS. A thorough site survey of all system support requirements should be conducted for the Technical Implementation Plan that the Components develop for each of their modern DCPDS deployment sites. This site survey is used to determine and size the support system hardware, software, and communication requirements based on such factors as serviced population and associated database sizes for each RSC, CSU, and satellite personnel office expected to operate the modern DCPDS. The technical contractor conducts the "Operational Certification" which is the final step of the Technical Implementation Plan for standing up a RSC.

5.2.2.2 Equipment Requirements

Minimum equipment size and configuration requirements needed to support the modern DCPDS for the Components are listed in the Operational Certification Guide or issued by CPMS memoranda as updates. The Technical Implementation Plans, developed by the Components for each of their RSCs, are used to formally identify system support factors such as RSC, CSU, and satellite personnel office modern DCPDS user requirements, quantity and configuration of equipment, equipment POCs, equipment location, user training, and conversion from existing systems. Components are responsible for identifying their own modern DCPDS support requirements at their respective RSCs, CSUs, and satellite personnel offices. Requirements must be established and supporting documents and contracts must be prepared for life cycle maintenance of support equipment in accordance with the Systems Maintenance Plan. System support POCs at each RSC, CSU, and satellite personnel office must promptly elevate, through their chain of command, any unresolved critical system support equipment problems. Reports of unresolved problems are considered critical if those problems adversely affect the deployment schedule for any site.

5.3 Deployment Working Group

5.3.1 Purpose of Deployment Working Group

The modern DCPDS Deployment Working Group consists of representatives from CPMS, the technical contractor, and each DoD Component. The purpose of this working group is to develop a common understanding of the myriad of modern DCPDS deployment requirements affecting the deployment program, and to promote cooperation, communication, and synergy among all deployment POCs. The Deployment Working Group meetings will cross-feed information among the technical contractor, CPMS, and Components regarding deployment planning concerns, deployment schedules, data conversion, site preparation, system deployment requirements, and any related matters affecting deployment.

5.3.2 Working Group Composition

The CPMS Program Manager for modern DCPDS deployment planning chairs the Deployment Working Group. This group will meet, as necessary, until deployment is complete. All members of the Deployment Working Group should have a working knowledge of the modern DCPDS deployment and installation strategy, computer terminology, and all plans associated with this program. These include, but are not limited to, the Security Support Plan, Training Support Plan, Configuration Management Plan, Systems Maintenance Plan, Operational Certification Guide, and their Component deployment schedules.

5.3.3 Information Exchange

The Deployment Working Group will exchange information at the periodic meetings, brief the deployment planning status of each Component, and report and discuss any problems that could delay the modern DCPDS deployment. All information generated from the working group will be disseminated through the Component deployment representatives to their site POCs. Information flow from the site POCs will follow the same route in reverse.

6. MIGRATION FROM LEGACY DCPDS TO MODERN DCPDS

6.1 Legacy DCPDS and PPI Suite Deactivation

The legacy DCPDS and the PPI suite will cease operation once the modern DCPDS is deployed on-site. The legacy DCPDS and PPI suite will continue to support each RSC, assigned CSUs, and satellite personnel offices waiting for deployment of the modern DCPDS. A region attains full modern DCPDS operational status at the regional office and associated deployment sites when all supporting hardware, software, and communications connectivity are in place and certified as fully operational. Full operational status must also include all modern DCPDS transaction interfaces with other functional areas, such as pay. No RSC or assigned CSU may return to using the legacy

DCPDS or the integrated PPI suite after the modern DCPDS deployment starts and is certified as fully operational. Reverse conversion procedures are not being developed.

6.2 Termination of Legacy DCPDS Operational Support

Discontinuance of the legacy DCPDS and PPI suite mainframe computer operational support will be necessary when the modern DCPDS is deployed to a region. Exceptions to this rule may be made for assigned CSUs or satellite personnel offices. Exceptions may also include sites not ready for the deployment, or sites that recently joined the region but must continue to use the legacy system and PPI suite. Requests for continued use of the legacy DCPDS and PPI suite must be immediately brought to the attention of CPMS for an evaluation of the effect on the master DoD deployment schedule. Evaluation must be made before a deployment can begin to any region. Curtailment of business contracts, arrangements, and leases between the Components and support agencies (e.g. Defense Information Systems Agency (DISA)) for termination of mainframe computer and associated operational support of the legacy DCPDS and the PPI suite is the responsibility of the Components. The Components should notify their support agency (such as their servicing Defense Megacenter (DMC) within the Defense Information Systems Agency (DISA), or contracted company that currently provides their legacy DCPDS and PPI suite mainframe operational support) of the need to terminate their system support and associated contracts or agreements when the modern DCPDS is deployed. Components should develop “stairstep” plans in close coordination with their current legacy DCPDS support agency or company to shut down operational support of the legacy DCPDS for each deployment site in direct conjunction with their respective modern DCPDS deployment schedules. The Components must be aware that most support agencies, such as DISA, may require advance notice of 180 days or more to terminate the current software and hardware support level agreements. Deployment POCs are responsible for local coordination of data conversion requirements and actions between the technical contractor and their respective supporting agency or private firm prior to their legacy DCPDS and PPI suite support termination. Components are encouraged to include in their deployment schedules explanations of any serious risks associated with shutting down the legacy DCPDS and PPI suite support, and implementing the modern DCPDS at any particular deployment site.

6.3 Contingency Plans

Contingency plans are needed in the event RSCs, CSUs, and satellite personnel offices experience catastrophic facility, hardware, or software problems during or after deployment that prevent them from using the modern DCPDS. A CPMS Contingency Management Manual is available for use by all Components to facilitate their development of Continuity of Operation Plans (COOPs) for their own RSCs, CSUs, and satellite personnel offices. The Contingency Management Manual will provide guidance on the development, implementation, and maintenance of COOPs and disaster recovery plans to safeguard the hardware, software, and database associated with the modern DCPDS located at the RSCs, CSUs, and satellite personnel offices. The COOPs will help minimize the turmoil of modern DCPDS disruption in the event of a disaster, and facilitate survival and continuation of critical modern DCPDS support. The technical contractor will prepare a formal, comprehensive, and fully integrated COOP and associated set of procedures for the CMIS equipment, software, and operations located in the technical contractor's facility. See the CONOPS for additional information on the COOP and related development plans.

6.4 Partial Deployment of Modern DCPDS

The intent of this deployment program is to completely deploy the modern DCPDS to each region including the respective RSC, assigned CSUs, and satellite personnel offices concurrently during the scheduled period of deployment. However, during the modern DCPDS deployment, Components may have regions with one or more assigned CSUs and satellite personnel offices which cannot transition from the legacy DCPDS or the PPI suite to the modern DCPDS due to problems with system installation, site preparation, equipment, etc. Once the data conversion is successfully completed and the modern DCPDS is fully operational and certified for a region, use of the legacy DCPDS and the PPI suite by all assigned personnel offices within that region must cease. Sites, to which the modern system cannot be deployed when originally scheduled with their parent RSC, must be immediately rescheduled with CPMS for deployment. Components should consider using alternate RSC and CSU sites as contingency-processing sites for any assigned CSUs and satellite personnel offices experiencing initial modern DCPDS installation and operating problems. Alternate sites could also be used as a temporary solution to system downtime problems after the system is fully deployed to an entire region.

7. PERSONNEL ACTIONS MORATORIUM

Prior to deployment of the modern DCPDS to any RSC and associated CSU or satellite personnel office, deployment sites must evaluate and make preparations for pending and projected personnel action requests submitted by supervisors prior to deployment, and during or after deployment. All personnel offices and the supervisors and employees they support must be aware that a moratorium will be implemented during deployment on <u>all</u> automated civilian personnel action processing on the legacy DCPDS and the PPI suite, where used, until the modern DCPDS is fully operational for an affected region. Variations of these types of pending actions are addressed below with suggested solutions. Even though the Components must stop using the legacy system and the PPI suite when the data is baselined to begin data conversion and validation, these systems currently have the capability to remain operational long enough to authenticate the SF-50's and their printing resulting from the last end-of-day processing.

7.1 Controllable Projected Personnel Actions Pending in Legacy DCPDS at Time of Deployment

Personnel actions, which are pending in the legacy DCPDS and projected to consummate during the time the modern DCPDS is being deployed to a region, will not be converted to the modern DCPDS. These projected personnel actions must be deleted and reentered once the modern DCPDS is deployed to the region. The following are some but not all-inclusive examples of controllable personnel actions: merit promotions, resignations, retirements, reassignments, details, temporary appointments, and accessions. Automated processing of these and all categories of personnel actions on the legacy DCPDS and the PPI suite will be prohibited when deployment begins. If emergency personnel actions must be processed during deployment, the personnel office will have to manually prepare the actions and then retroactively enter them into the modern DCPDS database after deployment is completed. These actions also include Standard Form-50s (SF-50s) with future effective dates from the PPI suite, and separation and retirement actions where the employee has selected an effective date to occur during or after the deployment period. Deployment sites will not be permitted to process any pending personnel actions in the legacy DCPDS or the PPI suite which are scheduled to occur after modern DCPDS deployment has started in their assigned region. Automated personnel actions will not be entered into the modern DCPDS until it is fully operational and certified. A standard DESIRE will be developed and made available to all Components to allow reports to be run prior to the data conversion and to identify projected personnel actions that will occur during and after deployment is initiated. This DESIRE will permit the deployment sites to determine what action needs to be taken.

7.2 Processing Emergency Personnel Actions During Deployment

Proper deployment planning will reduce the need to process emergency personnel actions during deployment. Standard personnel actions that can be postponed until after deployment should not be planned during this period. Emergency personnel actions, which may have to be processed during deployment, will typically be those that cannot be predicted and must be processed immediately for timely payroll processing. By regulation, these types of actions cannot be rescheduled. Examples of these types of actions include, but are not limited to, leave without pay for more than 30 days, resignations, retirements, death, and disciplinary actions. Listed below are the emergency personnel actions approved for processing and transmission to the Defense Finance and Accounting Service (DFAS). If processing of these actions cannot be done until after the modern DCPDS is operational at a deployment site, then the only alternative may be to manually process them and retroactively enter them into the modern DCPDS after deployment. Manual processing of emergency personnel actions during the downtime period of a deployment is suggested only as an alternative to not processing these types of actions at all. Responsibility for deciding to manually process any emergency personnel action during a downtime period ultimately remains with the Component. With minimal downtime expected, and with proper personnel action planning for deployment, these types of actions should be the exception. For timely processing of any actions that affect payroll, a copy of every manually processed SF-50 for an emergency action must be immediately faxed to the servicing Defense Finance and Accounting Service (DFAS) office for their action. Each SF-50 transmittal must remind the servicing DFAS office that the SF-50 will be faxed to them. This reminder should be documented in writing and may be emailed or faxed to the servicing DFAS office. After the modern DCPDS becomes operational for the deployment site, all personnel actions that were manually processed during deployment must be input to the modern DCPDS. These sites must contact their servicing DFAS office to remind them that these actions will be input to the modern DCPDS and to expect a data flow from the modern DCPDS. This second reminder to DFAS will preclude double processing of pay actions by DFAS.

Acceptable Emergency Personnel Actions

100	Career Appt
101	Career – Conditional Appt
102	Career - Exec Assignment
103	Career - Exec Assignment - Conditional
104	Non- Career Exec Assignment
107	Emergency Appt
108	Term Appt – NTE
112	Term Appt – NTE Permanent
115	Temp Appt – NTE
120	O/S LTD Appt -
122	O/S LTD Appt NTE
124	Appt Status Quo
128	LTD Exec Assignment
140	Reins – Career
141	Reins Career Cond
142	SES Career Appt
143	Rein - SES Career
146	SES Non Career Appt
148	SES LTD Term Appt
149	SES LTD Emergency appt - NTE
150	CA Career Conditional Appt
151	CA Appt Career Appt
153	CA Appt – NTE
154	CA Term Appt – NTE
155	CA Reappt
170	Exc Appt
171	Exc Appt NTE
190	Provisional Appt
198	Interim Appt – Non Duty Status
199	Interim Appt
280	Place in Pay Status
292	Return to Duty (RTD)
293	Return to Pay Status
300	Retirement – Mandatory
301	Retirement – Disability
302	Retirement – Voluntary
304	Retirement - In Lieu of Invol Action
312	Resignation - In Lieu of Invol Action
317	Resignation
330	Removal
350	Death
351	Termination – Sponsor Relocating
352	Termination – Appt In (Agency)
353	Separation – Military
354	Termination – Disability

355	Termination – Expiration of Appt
356	Separation – RIF
357	Termination
385	Termination During Prob/Trial Period
386	Discharge
430	Placement In Non - Pay Status
450	Suspension – NTE
452	Suspension – Indefinite
460	LWOP – NTE
462	LWP – NTE
471	Furlough
472	Furlough – NTE
473	LWOP – Military
500	Conv to Career Appointment
501	Conv to Career Conditional Appointment
502	Conv to Career Exec Assignment
503	Conv to Career Exec Assignment Conditional
504	Conv to Non- Career Exec Assignment
507	Conv to Emergency Appt
508	Conv to Term Appt – NTE
512	Conv to Term Appt – Permanent
515	Conv to Appt – NTE
517	Conv to Summer Appt - NTE
520	Conv to O/S LTD Appt
522	Conv to O/S LTD Appt - NTE
524	Conv to Appt – Status Quo
528	Conv to LTD Exec Assignment
540	Conv to Reins – Career
541	Conv to Reins – Career- Conditional
542	Conv to SES Career Appt
543	Conv to Reins SES Career
546	Conv to SES Non -Career Appt
548	Conv to SES LTD -Term Appt NTE
549	Conv to SES LTD – Emergency Appt - NTE
550	Conv to CA Career – Cond Appt
551	Conv to CA Career – Appt
553	Conv to CA Appt – NTE
554	Conv to Term Appt – NTE
555	Conv to CA Reappt
570	Conv to Excepted Appt
571	Conv to Excepted Appt – NTE
590	Conv to Provisional Appt - NTE
713	Change to Lower Grade
762	Ext of SES Limited Appt - NTE
765	Ext of Term Appt – NTE
772	Ext Of Furlough – NTE

773	Ext of LWOP – NTE
866	Termination of Grade Retention

7.3 Uncontrollable Personnel Actions Pending in Legacy DCPDS During Deployment

These are personnel actions that are normally system-generated based on suspensed actions and there is no regulatory acceptable way to reschedule them. Examples of these include within-grade-increases (WIGIs), conversions to career status, separation of temporary appointments, return of employees from suspensions, termination of temporary promotions, and all actions taken because of reaching a not-to-exceed (NTE) date during deployment. There are some preparatory actions which deployment sites may take to minimize the occurrence of personnel actions suspensed to occur during deployment. Deployment sites are highly encouraged to determine if the anticipated NTE actions can be adjusted to consummate before or after the deployment. The WIGIs should be a minimal problem during deployment since WIGIs typically occur on ending pay periods. While manually-processed personnel actions should be kept to a minimum, the deployment sites may follow the recommended manual personnel processing procedures cited in paragraph 7.2 above, if required.

7.4 SF-52 Pipeline Actions Unconsummated in PERSACTION

Pipeline actions in the legacy DCPDS are SF-52 personnel action requests from managers that are in various phases of completion, such as filling vacancies, retirement, and separation actions, but which have or will have an effective date following the date deployment commences. All unconsummated SF-52 personnel action requests residing in PERSACTION at the time of deployment have to be manually reinitiated in the modern DCPDS after it becomes operational. Deploying sites are advised to minimize the number of SF-52s in the pipeline at deployment time.

7.5 Vacant Position Data

Vacant position data residing in the legacy DCPDS and PPI suite will be converted to the modern DCPDS upon deployment. Components must review their vacant positions and delete any invalid or otherwise unneeded positions prior to deployment. This validation is necessary to reduce the file size. Large files of invalid, vacant (unencumbered) positions will affect the length of time for data conversion.

8. TRAINING

CPMS has developed a Training Support Plan (TSP) that outlines the training requirements for the modern DCPDS. This plan includes training for testing and deployment of the modern DCPDS. The TSP is available on the CPMS web site at www.cpms.osd.mil/pmo/Tsp97b.doc or from the Regionalization and Systems Modernization Division staff at (703) 696-2775 or DSN 426-2775. An updated users guide is also being made available on the CPMS web site.

9. DATA CONVERSION

9.1 Data Conversion to Modern DCPDS

(See Appendix for data conversion details.)

9.2 Advanced Data Validation

Data validation of each deployment site's current database must be accomplished prior to system certification of the modern DCPDS for these sites. Components are encouraged to begin their data validation immediately, but no later than 120 days before the scheduled data conversion and deployment date for each site. This will preclude the "last minute" identification and correction of erroneous data that could adversely affect the timely completion of the system deployment and certification at these sites. Specific quantity and type of selected data to be validated is left to the discretion of the Components and can be accomplished using quality control DESIREs. Data selected for validation should be specific enough to represent a valid cross section of all of the deployment site's personnel records and data elements. The amount and type of data selected have a direct proportional effect on the success of the subsequent data conversion. Data validation is necessary to determine the existence of such data errors as incompatibility of current database content, length, or structure with that of the modern DCPDS, and current erroneous or unusable data. Components must anticipate and plan for their pre-deployment workload for both correction of data and entry of added data requirements (i.e., organizational relationships, position hierarchies, military supervisory positions, and user identifications). CPMS reserves the authority to delay deployment to any region if actions are insufficient to correct erroneous data which may cause the unscheduled delay or unreasonable duration of a deployment.

9.3 Status Six Records

A "status six" record is either a valid future-dated accession action (e.g., a career conditional appointment or change in appointing office (CAO)) or a past due accession action that rejected and was not fixed so that the action could consummate. If there are incomplete CAOs in the legacy DCPDS when conversion starts, they will not be converted to the modern DCPDS. The RSCs are encouraged to identify and clear these records before deployment. These records will be automatically dropped during the data conversion phase of deployment. Any reentry of these records will have to be done after the data conversion process and the completion of deployment.

9.4 Data Validation During Deployment

During the period of time while the data are being converted and validated by the technical contractor, and during the installation of the modern DCPDS at each deployment site, there will be downtime when processing will cease on both the legacy DCPDS and the PPI suite, where used. Data validation must occur at this time. See Figure 1 in Appendix for the data conversion and validation process. If the deployment sites cannot validate their database in advance, very limited data validation may be accomplished during the system deployment and personnel action processing startup period. Data capture, validation, and correction during this very short period of time exposes the deployment sites to serious risks of delaying system certification for the affected site and the remainder of the region to which it is assigned. Ideally, the data should be validated prior to the data conversion by the technical contractor.

9.5 Hierarchy Data in Modern DCPDS

9.5.1 Hierarchy Data Structure

The modern DCPDS is based upon two levels of hierarchy: organization and position. In applying this hierarchy structure to the modern DCPDS, the organizational hierarchy is taken to the individual Unit Identification Code (UIC) or the Personnel Authorization System (PAS) code. While the actual levels differ from Component to Component, whatever level the Component decides to use for their UIC/PAS level is where organizational hierarchy will end and position hierarchy will begin.

9.5.2 Organization Hierarchy Data Maintenance

The UIC/PAS level information will be the same for all users of the modern DCPDS. There will be only one hierarchy and it will be centrally maintained. The initial UIC/PAS hierarchy is being built by the technical contractor prior to data conversion with information provided from the Components. Components will be responsible for providing changes to the UIC/PAS hierarchy to a central maintenance location (TBD). Changes are expected to be made and passed back for field level use within a few days from the initial request date.

9.5.3 Position Hierarchy Data Maintenance

The position hierarchy will start with the senior position in the UIC/PAS organization level. Subordinate positions will be attached to the senior level. The initial hierarchy will be built during conversion of legacy data. The procedure to build the position hierarchy is contingent upon a clearly aligned local Table 30 (currently used only with legacy DCPDS) and the addition to the legacy database of intervening military positions in the chain of command. Even with a completely logical Table 30 design and all military positions being entered, we expect only an 85-90% accuracy in the initially-built position hierarchy. Situations with multiple supervisors in the same grade level of varying pay plans do not support automated decisions. There will be some level of corrective action required during the conversion process to properly complete the position hierarchy. Position hierarchies will be maintained at the RSC level after deployment. Delegating data entry for the position hierarchy below the regional level will be a Component decision. While position hierarchy maintenance is not complex, the relative ease with which the hierarchy may be unintentionally changed suggests that some restriction on access to this data is appropriate.

9.5.4 Military Position Hierarchy Data

Military positions that have supervisory controls over civilian employees need to be included in the position hierarchy data build. Failure to include the military positions will limit the members' ability to access the system and will provide viewers with an incomplete picture of position hierarchy. Where the military position is key to the chain of command, it is possible that hierarchy breaks could occur. The result will be incomplete reporting and system access to any supervisor or senior manager to the point of a hierarchy break. Military positions have a minimum of data and do not have to be maintained with incumbent information.

9.6 Historical Data

9.6.1 Historical Data Capture

CPMS deployment program plans do not include the conversion of historical data from the A**LOA tapes to the modern DCPDS. The deployment plan only calls for capturing the last data dump of historical data from the legacy DCPDS on A**LOA tapes immediately after use of the legacy DCPDS ceases and prior to executing the data conversion for deployment of the modern DCPDS. Components should be aware that A**LOA tapes will no longer be retrievable from the legacy DCPDS for any sites which have been converted to the modern system.

9.6.2 Historical Data Conversion

The conversion of historical data from the legacy DCPDS to the modern DCPDS is excluded from this deployment plan. Only the conversion of current employee data to the modern DCPDS will be supported and funded by the DCPDS modernization program. After that initial conversion, the modern DCPDS will then begin accumulating historical data in its own relational database management system (RDBMS) with data updates as a result of processing personnel actions after deployment.

10. CONFIGURATION MANAGEMENT (CM)

During deployment of the modern DCPDS and its operation, CM is necessary to identify, document, and control the functional and physical characteristics of the modern DCPDS, to establish baselines and control changes to those baselines, and to document the configuration of the system. CM control ensures that the modern DCPDS is responsive to operational needs, effectively satisfies mission requirements, and can be efficiently supported. See the Configuration Management Plan for associated details on such matters as software configuration identification, configuration status accounting, and configuration control of the software supporting the modern DCPDS. The CM plan contains guidance on patches and software changes, both system and functional, during modern DCPDS initial deployment and for life cycle maintenance. Local system and security administrators must be alert to any proposed changes to the hardware or software configuration supporting the modern DCPDS, which may affect the security of the database.

10.1 Changes to Operating System Hardware or Software

Any changes to the operating system hardware or software configuration at any site prior to or after modern DCPDS deployment, without certification or recommendation from the technical contractor, could adversely affect the operation of the modern DCPDS. Likewise, any addition of uncertified software (i.e., not certified by the technical contractor) could adversely alter the operation of the modern DCPDS. Components will be responsible for any automated personnel processing delays or problems due to their uncertified alterations, installations, or additions to the hardware or software configuration which adversely alter the operation of the modern DCPDS. If the RSC, CSU, or satellite personnel office POC for configuration management has any doubt or questions prior to making any changes to their operating system hardware or software, they are encouraged to elevate their concerns to their Component project manager or the technical contractor.

10.2 Operating System Software Version Control

Components must ensure that only correct versions of the operating system software (i.e., certified by the technical contractor) are loaded on computer hardware which are purchased to operate the modern DCPDS. Using the latest system software version does not necessarily ensure that it is the correct version. For example, some acquisition contracts used by the Components may require the vendors to provide the latest version of the operating system to be shipped with the ordered computer hardware. In most instances, this would be the best method of ordering the operating system when purchasing computer hardware. However, this may pose problems if the newly purchased computer hardware will be delivered containing a more recent version of the operating system software that is not compatible with the modern DCPDS. Components are cautioned to verify with the technical contractor that only the correct (i.e., not necessarily the latest) version (as certified by the technical contractor) of the operating system software is loaded on the computers used to operate the modern DCPDS. The technical contractor will publicize the exact software versions that will be deployed and certified as inter-compatible. During deployment, the tapes uploaded to the regional server contain the required software.

11. SECURITY

11.1 Security Goals

The modern DCPDS security program goal is for the protection, integrity, confidentiality, and availability of the modern DCPDS and associated data. Data processed by the modern DCPDS is considered to be sensitive-unclassified which necessitates controlled access to both it and the modern DCPDS. Deployment site security administrators, who may also be referred to as Information System Security Officers (ISSOs), or Computer System Security Officers (CSSOs), must ensure compliance with all security requirements referenced in the Security Authorization Agreement (SSAA). Before modern DCPDS deployment, Components must ensure each deployment site ISSO or CSSO has implemented all required security controls, policies, and procedures to limit access to the modern DCPDS to authorized users, and to prevent unauthorized modification, destruction, or disclosure of sensitive data processed by the modern DCPDS. The SSAA identifies details on such matters as procedures for implementing the security requirements for the modern DCPDS operation. It also outlines modern DCPDS life-cycle plans for task accomplishment, identifies detailed tasks that must be performed to maintain system security, and describes security plans for transitioning from legacy DCPDS to the modern DCPDS. Local system and security administrators must be alert to any proposed changes to the hardware or software configuration supporting the modern DCPDS, which may affect the security of the database.

11.2 Security References

All data processing, transmission, retrieval, and computer and communication resources associated with the modern DCPDS must be managed and administered according to applicable DoD security directives, the Privacy Act of 1974, and published modern DCPDS SSAA. The modern DCPDS SSAA explains the details of the security directives to be followed for the use, maintenance, and administration of the modern DCPDS. The modern DCPDS security protection program requirements apply to all modern DCPDS end users at the Components, RSCs, CSUs, and satellite personnel offices. End users include all personnelists, managers, database administrators, systems administrators, and other staff members who use the modern DCPDS.

11.3 User Access to Modern DCPDS

Prior to deployment of the modern DCPDS, Component security POCs or equivalent security administrators must establish their modern DCPDS authorization and access control processes in accordance with the requirements detailed in the modern DCPDS SSAA and other applicable security directives. Security administrators are reminded that the users’ job requirements provide the essential basis for access to the modern DCPDS following “least privilege” or “need to know” security concepts. These security concepts dictate that modern DCPDS and CMIS users are limited only to the minimum viewing and access privileges that they need for their jobs. Local security administrators will issue controlled user identifications (IDs) and passwords for each authorized user of the modern DCPDS. Individual, unique passwords will be established when the user first logs into the database application or server. All UNIX system and Oracle HR designated default passwords delivered with the Oracle HR software or the server platform will be deleted.

11.3.1 Preparation for User Access to Data in the Modern DCPDS

In preparation for modern DCPDS deployment, Component security administrators will be responsible for controlling Component, RSC, CSU, and satellite personnel office user access to the modern DCPDS. Components may further delegate modern DCPDS security administration. Component security administrators of the modern DCPDS are responsible for identification of user IDs and passwords within their organization.

11.3.2 User Access to the Corporate Management Information System (CMIS)

Access to the CMIS database, located at the technical contractor's facility, will follow the security concepts explained in the SSAA. The technical contractor's system administrator will support Component user access to the CMIS database in coordination with the Component security administrators and personnel managers. The technical contractor will create all accounts for Component security administrators for CMIS access. Accordingly, Component security administrators will create user IDs and passwords for each authorized Component user. Prior to account creation, the appropriate personnel manager will approve Components' authorized users. This approval will be confirmed through documentation with the security administrator.

11.4 Preparation for CMIS Security Administrator Accounts and User Security Training

In preparation for access to the CMIS, the technical contractor system administrator will create security administrator accounts for each Component. Component security administrators will provide system security training to their CMIS users prior to the creation of user accounts by the technical contractor or the Component security administrators. Components will be required to register the user's password on an as needed basis.

11.5 Component Initial User Access Required Actions

Prior to IOC, Component security administrators must receive training on the use of the modern DCPDS to be able to create accounts for authorized users. Personnel managers will work with their Component security administrators to identify authorized users, access requirements, and responsibilities. This includes both access to local database and application servers and Component access to the CMIS database at the technical contractor's facility.

11.6 Certification and Accreditation at RSC and CSU Sites

RSC and CSU security administrators will ensure risk analysis is conducted at their site in accordance with the modern DCPDS SSAA. All sites require certification and accreditation by the local Designated Approving Authority (DAA) prior to deployment.

12. DEPLOYMENT PLAN MAINTENANCE

Changes and updates to this plan will be made to meet new or revised deployment requirements. Distribution of these changes will be made to the Components during the periodic meetings of the deployment working group, described previously in this plan, or via correspondence, whichever method is the most prompt. Local reproduction of this document in whole or in part is authorized. Limited distribution of this document, in whole or in part, to only US Government agencies for installation, test, and deployment use is authorized. Other requests for this document will require written approval from CPMS.

13. DOCUMENTS REFERENCED IN DEPLOYMENT PLAN

Document	OPR or Document Source
Training Support Plan	CPMS
Deployment Schedule	CPMS
Sustainment CONOPS	CPMS
Modern DCPDS User Documentation	CPMS
Technical CONOPS	Technical contractor
Security Support Plan	Technical contractor
Configuration Management Plan	Technical contractor
Contingency Management Guide	CPMS
Security Features Users Guide	Technical contractor
Maintenance Support Plan	Technical contractor
IOC Certification Checklist	Technical contractor
Communication Support Plan	Technical contractor
AFOTEC OT&E Plan	AFOTEC
Technical Risk Management Plan	Technical contractor
Deployment Checklist	Deployment Preparation and Implementation Guide
Equipment Test Plan	Component Site
Site Preparation Plan	Component Site
Technical Implementation Plan	Component Site

APPENDIX A – SAMPLE DEPLOYMENT DURING ANY MONTH

SUN	MON	TUES	WED	THUR	FRI	SAT
Start Pay Period			1	2 STOP ~ Last day to process personnel actions on legacy DCPDS ~ Start legacy termination process	3 "d" day ~ Complete Legacy termination process ~ TC starts data capture & conversion	4 ~ CPMS deployment team arrives ~ TC continues conversion ~ RSC POCs at TC for prescreening process
5 ~ TC data conversion continues ~ RSC POCs correct conversion rejects	6 ~ RSC POCs correct conversion rejects continues ~ Create Oracle secure userids	7 ~ Create Oracle secure userids continues	8 ~ Create Oracle secure userids continues	9 ~ Install deployment system at TC ~ Verify conversion database	10 ~ Miscellaneous configuration changes	11 End pay period ~ Create deployment tapes ~ TC Deployment Team arrives at RSC
12 Start pay period ~ Load region ~ Establish CSU ~ Establish RESUMIX Load	13 ~ Create userids ~ Install network printers ~ Define routing groups ~ Initiate recurring processes	14 ~ Continue… ~ Create userids ~ Install network printers ~ Define routing groups ~ Initiate recurring processes	15 ~ Continue… ~ Create userids ~ Install network printers ~ Define routing groups ~ Initiate recurring processes	16 ~ Full Region capability	17 ~ Certify modern DCPDS Operational	18
19	20	21	22	23	24	25 End pay period
26 Start pay period	27	28	29	30	31	

APPENDIX B – GLOSSARY OF TERMS AND ABBREVIATIONS

ALOA**	Legacy DCPDS Tape containing Database and Table Information
AFOTEC	Air Force Operational Test and Evaluation Center
API	Application Process Interface
AQP	Acquisition Program
CAN	Campus Area Network
CIVMOD	Civilian Modernization
CONOPS	Concept of Operations
CONUS	Continental US
COTS	Commercial Off the Shelf
CM	Configuration Management
CMIS	Corporate Management Information System
CPMS	Civilian Personnel Management Service
CSSO	Computer System Security Officer
CSU	Customer Support Unit
DAA	Designated Approving Authority
DCPDS	Defense Civilian Personnel Data System
DFAS	Defense Finance and Accounting Service
DID	Data Item Description
DISA	Defense Information Systems Agency
DMRD	Defense Management Report Decision
DoD	Department of Defense
DOS	Disk Operating System
DSN	Defense Switched Network
EOD	End-of-Day
FAS	Field Advisory Services
FOC	Full Operating Capability. (FOC is attained when all DoD sites have moved from the legacy system.)
FTP	File Transfer Protocol
HP UNIX	Hewlett Packard Operating System
HR	Human Resources
IAW	In accordance with
ICMIS	Interim Corporate Management Information System

ID	Identification Designator. Normally referenced as "user ID".
ISSO	Information System Security Officer
IOC	Initial Operating Capability. (IOC is that point in time when the modern system is installed and first begins operating in preparation for the Operational Test and Evaluation (OT&E) phase.)
LAN	Local Area Network
MAIS	Major Automated Information System
MAISRC	Major Automated Information System Review Council
MAN	Metropolitan Area Network
NTE	Not to exceed
Oracle HR	Oracle Human Resources
OT&E	Operational Test and Evaluation
PAS	Personnel Authorization System
PBD	Program Budget Decision
PDM	Program Decision Memorandum
PERSACT	Personnel Action (One of several systems in the Integrated PPI suite)
POC	Point of Contact
POI	Personnel Office Identifier
PPI	Personnel Process Improvement
PPRS	Promotion Placement Referral System
PSM	Personnel System Manager
QOT&E	Qualification Operational Test and Evaluation
RESUMIX	COTS Resume (staffing) system
RSC	Regional Service Center
SA	Site Administrator
SF-XX	Standard Form- (Form type followed by a form number such as 50 or 52)
SDC	Software Distribution Center
SQL	Structured Query Language
SQT	Systems Qualification Test
TBD	To be determined
TRMP	Technical Risk Management Plan
TSP	Training Support Plan
UIC	Unit Identification Code
WIGI	Within Grade Increase

APPENDIX C – TECHNICAL DEPLOYMENT STRATEGY

1. Introduction

This appendix outlines the technical deployment strategy for both the modern DCPDS and the Corporate Management Information System. Actual deployment begins with the standup of the OT&E sites and ends with the last legacy DCPDS site being converted to the modern DCPDS. Phased deployment of sites with the modern DCPDS will essentially require some regions, or portions of regions, to be operational in both the legacy DCPDS and modern DCPDS simultaneously.

2. Purpose

Provide strategic information and outline the technical solution for deployment execution.

3. Scope

This annex applies during the establishment of the OT&E sites as well as full deployment of the modern DCPDS to all sites. This plan covers conversion of the legacy system from start of deployment until it is fully transitioned to the modern DCPDS for life-cycle support.

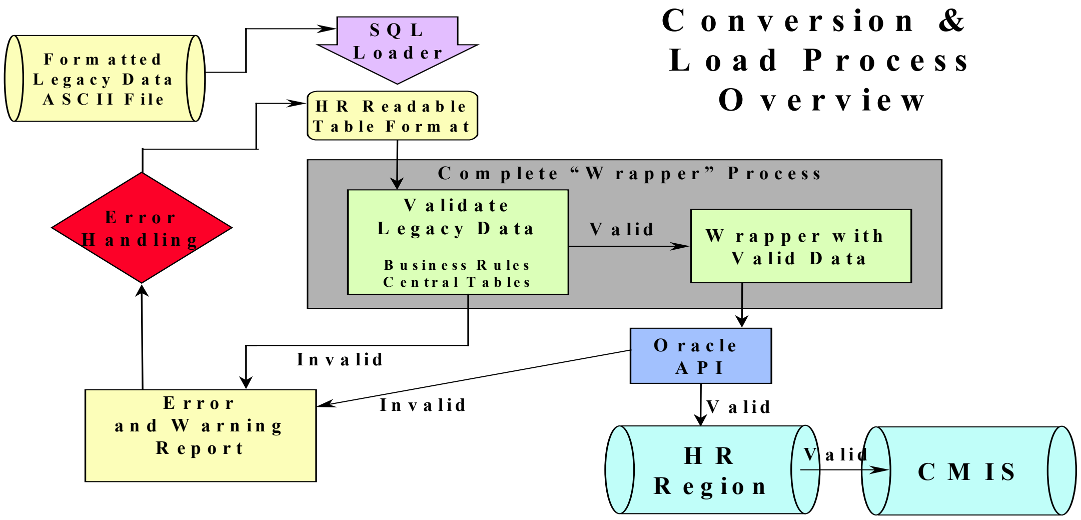
4. Risk Identification

Refer to the Technical Risk Management Plan (TRMP) which outlines risk identification.

5. Technical Deployment Strategy

Each region's deployment will be accomplished from the final legacy post end-of-day dump tape. The objective is to deploy all regions to the modern DCPDS with minimum down time. Figure 1 below outlines this process, reflecting that legacy data will be run through a Structured Query Language (SQL) Loader and staged in Oracle conversion tables. Next step will be to run the data through a Wrapper Process that is a collection of PL/SQL packages with conversion scripts. The process will validate, convert, and load the legacy data through script coding. The data will be validated on a simulated region server. At the same time, the region data will be established on the CMIS. As a region is converted, rejects are expected to occur due to incompatibility of legacy data with modern DCPDS, e.g., zeros for a date field. Rejects will be handled as outlined in figure 1 below.

Figure 1 – Conversion & Load Process



6. Processing Sequence

6.1 Receive file of data items to be converted and updated into modern DCPDS database.

6.2 Run update file through SQL Loader and stage data in Oracle conversion tables.

6.3 Data items are processed through a wrapper (validate, convert, and load).

6.4 Wrapper sends data items through Application Process Interface (API) for insertion in the modern DCPDS.

7. Wrapper Definition

7.1 A wrapper is a collection of PL/SQL packages containing conversion scripts.

7.2 Scripts are created by the technical contractor conversion team based on input from the technical contractor development team.

7.3 Legacy data items are retrieved, validated, converted, and loaded through script coding.

8. Data Reject Handling

8.1 A mock database conversion will be performed prior to deployment, and a reject listing will be provided to the Component to correct the necessary legacy data. When the time for actual deployment occurs, the conversion is executed, and if the errors amassed are too large to correct with the described process, the deployment will be delayed until the errors are reduced to an amount that can be accomplished in the time allotted for the database conversion process.

8.2 When the actual conversion is accomplished, staging files will be available for the tables that are to be loaded. As with the mock conversion, a reject listing will be provided to identify any remaining errors. The staging file will have both good and bad records. The bad records will not have an ID indicating that they were not processed, but will have error messages in the error columns. When reprocessing, the errors will be voided and the data revalidated. The good records from this process will be applied to the modern DCPDS database.

8.3 When the Component representative determines what the correct data is, he/she will provide the information to the technical contractor. This correct data will then be applied using SQL procedures to the bad record file to update the modern DCPDS database.

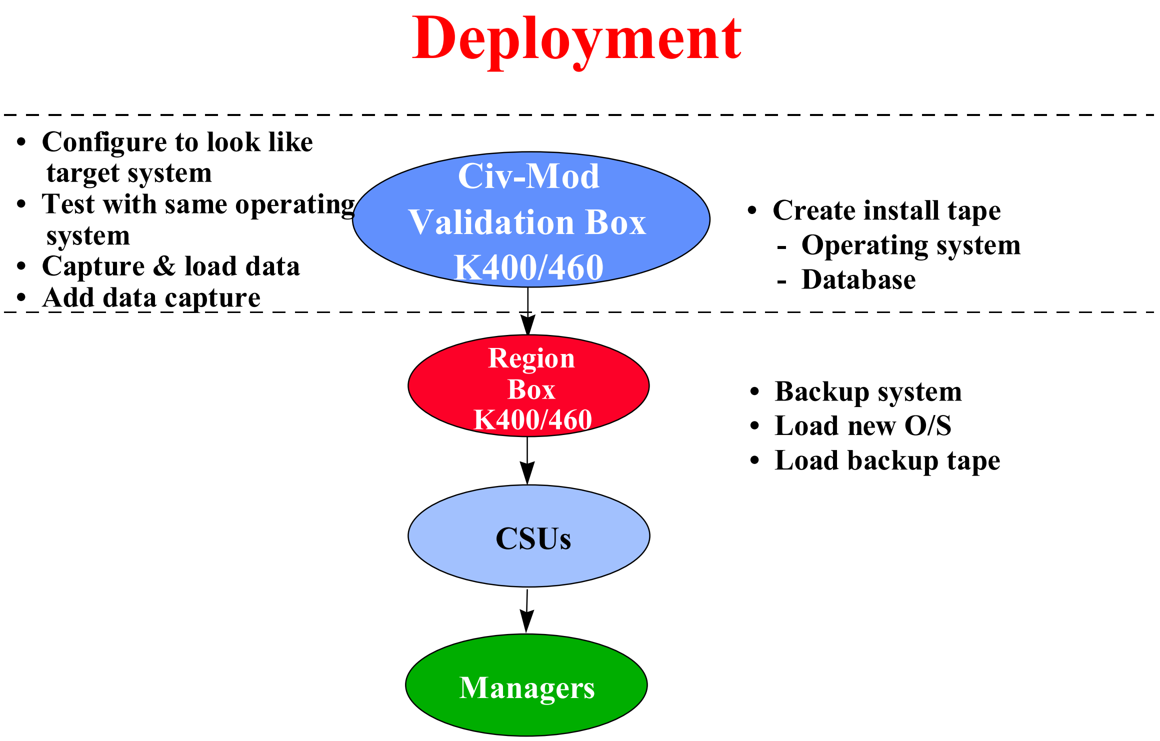
8.4 When all the records are fixed and ready for implementation, the validated file will be used both for the Region database and to build the CMIS database.

8.5 If there are erroneous or invalid data that pass through the mock conversion, and this correction process, a review of these cases will be made on an individual basis. The first option will be to see if mistakes can be fixed by using the modern DCPDS application. If this process cannot be used, then an updated SQL code will be written to correct the database.

9. Deployment

Figure 2 below outlines the deployment process. The converted regional database will be located on a validation server within the technical contractor's facility and will be configured exactly like the server of the region being deployed. The system will be tested to ensure valid operation. The Component deployment site is expected to validate the database. Once the validation is completed, a tape will be produced containing the operating system and database. At this point, the technical deployment team will hand carry the tape and the backup tape to the region for implementation.

Figure 2 - Deployment Process



10. Detail Specifications

For OT&E, the Oracle secure user accounts for managers/supervisors will be created at the technical contractor facility using Mercury Winrunner and Loadrunner. Encrypted userids and password will be provided to the POC at the region. Personnelists and "secure" external accounts will be established after the HR database has been deployed.

11. Legacy History Data Conversion

The CDA is developing an action plan and process to convert each Component's last regional database (at time of deployment) to an Oracle relational database. The purpose of this file is to provide a legacy history file, which can be addressable with modern DCPDS retrieval tools following deployment. This plan will provide the conversion of prior legacy history files (A**LOA tapes) and stand-alone systems such as headquarters-level files. Upon completion, this plan provides the proposed methodology and estimated cost, by Component, to accomplish this conversion. CPMS considers this process a DCPDS legacy requirement, not a modernization issue.